Eiropas Ekonomikas un sociālo lietu komitejas atzinums par tematu "Priekšlikums Eiropas Parlamenta un Padomes direktīvai par pasākumiem, kas nodrošinātu vienādi augsta līmeņa tīklu un informācijas drošību visā Savienībā"

COM(2013) 48 final – 2013/0027 (COD)

(2013/C 271/25)

Ziņotājs: ***McDONOGH* kgs**

Padome 2013. gada 21. februārī un Eiropas Parlaments 2013. gada 15. aprīlī saskaņā ar Līguma par Eiropas Savienības darbību 114. pantu nolēma konsultēties ar Eiropas Ekonomikas un sociālo lietu komiteju par tematu

"Priekšlikums Eiropas Parlamenta un Padomes direktīvai par pasākumiem, kas nodrošinātu vienādi augsta līmeņa tīklu un informācijas drošību visā Savienībā"

COM(2013) 48 final – 2013/0027 (COD).

Par Komitejas dokumenta sagatavošanu atbildīgā Transporta, enerģētikas, infrastruktūras un informācijas sabiedrības specializētā nodaļa savu atzinumu pieņēma 2013. gada 30. aprīlī.

Eiropas Ekonomikas un sociālo lietu komiteja 490. plenārajā sesijā, kas notika 2013. gada 22. un 23. maijā (22. maija sēdē), ar 163 balsīm par, 1 balsi pret un 5 atturoties, pieņēma šo atzinumu.

1. **Secinājumi un ieteikumi**

1.1 Komiteja pieņem zināšanai ierosināto direktīvu, kas jāskata plašākā kontekstā saistībā ar nesen publiskoto kiberdrošības stratēģiju ([1]), kurā izklāstīts visaptverošs redzējums attiecībā uz tīklu un informācijas drošību (TID) nolūkā garantēt drošu digitālās ekonomikas izaugsmi, vienlaikus popularizējot tādas Eiropas vērtības kā brīvību un demokrātiju.

1.2 EESK atzinīgi vērtē šo direktīvas priekšlikumu, kura mērķis ir Eiropas Savienībā nodrošināt vienādi augstu TID līmeni. Lai varētu pabeigt digitālā vienotā tirgus izveidi un garantēt netraucētu darbību iekšējā tirgū kopumā, TID saskaņošanai un pārvaldībai Eiropas līmenī ir būtiska nozīme. Komiteja ir vienisprātis ar Komisiju, ka TID kļūmes var nodarīt milzīgu kaitējumu tautsaimniecībai un iedzīvotāju labklājībai. Tomēr ierosinātā direktīva nav uzskatāma par šī kritiskā jautājuma risināšanai pietiekami iedarbīgu likumdošanas instrumentu, kā būtu vēlējusies Komiteja.

1.3 Ārkārtīgi lielu vilšanos Komitejai sagādā fakts, ka daudzās dalībvalstīs nav nekādu panākumu reālā TID īstenošanā valsts līmenī. EESK izsaka dziļu sarūgtinājumu par šo rīcības trūkumu, kas paaugstina draudus iedzīvotājiem un negatīvi ietekmē digitālā vienotā tirgus izveidi. Visām dalībvalstīm nekavējoties būtu jārīkojas, lai nodrošinātu neizpildīto TID saistību ievērošanu.

1.4 Šis progresa trūkums rada vēl vienu digitālo plaisu starp elitāro grupu, kurā TID ir augstā līmenī, un mazāk attīstītajām dalībvalstīm. Šādas atšķirības apgrūtina uzticēšanos un ES līmeņa sadarbību TID jomā, un, ja vien steidzami netiks mazinātas, tās var radīt iekšējā tirgus problēmas, kuru pamatā būs dalībvalstu atšķirīgās spējas.

1.5 Kā norādīts iepriekšējos atzinumos ([2]), EESK uzskata, ka pagaidu un brīvprātīgi pasākumi nav iedarbīgi un ka ir jānosaka stingras reglamentējošas dalībvalstu saistības nodrošināt Eiropas TID saskaņotību, pārvaldību un piemērošanu. Diemžēl, pēc EESK domām, aplūkojamais direktīvas priekšlikums nenodrošina skaidru un nepārprotamu tiesisko regulējumu, kāds šobrīd ir vajadzīgs. Komiteja uzskata: lai sasniegtu nepieciešamo vienādi augsto TID līmeni, iedarbīgāka par direktīvu būtu regula, kurā būtu skaidri noteiktas dalībvalstīm obligāti izpildāmās prasības.

1.6 Par spīti Eiropas Komisijas iecerei pieņemt deleģētos aktus, ar kuriem atsevišķu direktīvas daļu ieviešanā nodrošināt zināmu nosacījumu vienotību, Komiteja vērš uzmanību uz to, ka ierosinātajā aktā trūkst standartu, skaidru definīciju un kategorisku prasību, tāpēc kritiski svarīgo elementu interpretēšanā un transponēšanā dalībvalstīm dots pārāk daudz rīcības brīvības. Komiteja vēlētos, lai tiesību aktā būtu daudz precīzāk definēti standarti, prasības un procedūras, kas jāievēro dalībvalstīm, publiskajām iestādēm, tirgus dalībniekiem un galveno interneta pakalpojumu nodrošinātājiem.

([1]) "Atvērta un droša kibertelpa", JOIN (2013) 1.

([2]) EESK atzinums "Informācijas kritiskās infrastruktūras aizsardzība", OV C 255, 22.9.2010., 98. lpp., un "Direktīva par uzbrukumiem informācijas sistēmām", OV C 218, 23.7.2011., 130. lpp.

1.7 Lai Eiropas Savienībā varētu formulēt un īstenot stingru TID politiku, Komiteja ieteiktu izveidot ES līmeņa iestādi, kas atbildētu par TID un būtu līdzīga aviācijas nozares centrālajai iestādei (*EASA*) ([3]). Šī struktūra izstrādātu standartus un uzraudzītu visu TID aspektu īstenošanu Savienībā — no drošu termināliekārtu sertifikācijas un lietošanas līdz tīkla un datu drošībai.

1.8 EESK ļoti labi apzinās, ka mākoņdatošanas ([4]) ieviešana Eiropā palielina draudus kiberdrošībai un datu aizsardzībai. Komiteja uzskata, ka ierosinātajā tiesību aktā būtu skaidri jānorāda īpašas papildu drošības prasības un pienākumi mākoņpakalpojumu sniegšanai un lietošanai.

1.9 Lai TID jomā būtu iespējama pienācīga pārskatatbildība, tiesību aktā būtu skaidri jānosaka, ka struktūrām, kurām ierosinātā direktīva uzliek pienākumus, ir tiesības prasīt atbildību no programmatūras un aparatūras piegādātājiem, ja to produktiem vai pakalpojumiem bijuši tādi defekti, kuri kļuvuši par TID problēmu tiešu cēloni.

1.10 EESK aicina dalībvalstis pievērst īpašu uzmanību TID zināšanu un kiberdrošības prasmju palielināšanai mazajos un vidējos uzņēmumos (MVU). Turklāt Komiteja vērš Komisijas uzmanību uz "hakeru konkursu" panākumiem, ko tie guvuši ASV ([5]) un dažās ES dalībvalstīs ([6]), vairojot izpratni par kiberdrošības problēmām un audzinot nākamo TID profesionāļu paaudzi.

1.11 Ņemot vērā to, cik svarīgi visās dalībvalstīs ievērot Eiropas Savienībā pieņemtos tīkla un informācijas drošības noteikumus, EESK aicina Komisiju apsvērt, kādu daudzgadu finanšu shēmas finansējuma daļu varētu novirzīt TID prasību ievērošanai, lai palīdzētu tām dalībvalstīm, kam vajadzīgs finansiāls atbalsts.

1.12 Lai Eiropa spētu neatpalikt strauji mainīgajā kiberdraudu vidē, par vienu no galvenajām prioritātēm ES Pētniecības un inovācijas pamatprogrammā "Apvārsnis 2020" būtu jānosaka izdevumi TID tehnoloģiju jomas pētniecībai, attīstībai un inovācijai.

1.13 Lai būtu skaidrāks, kurām struktūrām ierosinātajā tiesību aktā paredzēta juridiska atbildība, EESK aicina visām dalībvalstīm noteikt prasību publicēt tiešsaistē pieejamu sarakstu, kurā būtu ietvertas visas struktūras, uz kurām attiecas direktīvas noteikumi par riska pārvaldību un ziņošanu. Šāda pārredzamība un publiska pārskatatbildība vairotu uzticēšanos un sekmētu noteikumu ievērošanu.

1.14 Komiteja vērš Komisijas uzmanību uz daudzajiem iepriekšējiem EESK atzinumiem par tīklu un informācijas drošību, kuros apskatīti tādi jautājumi kā, piemēram, drošas informācijas sabiedrības nepieciešamība un kritisko infrastruktūru aizsardzība ([7]).

2. **Komisijas priekšlikuma kopsavilkums**

2.1 Ierosinātā TID direktīva publicēta līdz ar ES kiberdrošības stratēģiju, kuras mērķis ir stiprināt informācijas sistēmu noturību, mazināt kibernoziegumu skaitu, sekmēt ES starptautisko kiberdrošības politiku un kiberaizsardzību, kā arī pilnveidot rūpnieciskos un tehnoloģiskos resursus kiberdrošībai, vienlaikus sekmējot pamattiesību un citu ES pamatvērtību ievērošanu.

2.2 TID uzdevums ir aizsargāt internetu un citus tīklus, informācijas sistēmas un saistītos pakalpojumus, uz kuriem balstās mūsu sabiedrības funkcionēšana. TID ir būtiski svarīga, lai iekšējais tirgus varētu darboties bez traucējumiem.

2.3 Pilnībā pēc brīvprātības principa veidotā pieeja, ko ES līdz šim izmantojusi, negarantē pietiekamu aizsardzību pret TID apdraudējumu. Ar pašreizējām TID spējām nepietiek, lai spētu neatpalikt strauji mainīgajā kiberdraudu vidē un visās dalībvalstīs nodrošinātu vienlīdz augstu aizsardzības līmeni.

([3]) Eiropas Aviācijas drošības aģentūra (http://easa.europa.eu/).

([4]) EESK atzinums "Mākoņdatošana (*cloud computing*) Eiropā", OV C 24, 28.1.2012., 40. lpp., un "Mākoņdatošanas potenciāla atraisīšana Eiropā", OV C 76, 14.3.2013., 59. lpp.

([5]) http://www.nytimes.com/2013/03/25/technology/united-states-wants-to-attract-hackers-to-public-sector.html?pagewanted=all&_r=0

([6]) http://www.bbc.co.uk/news/technology-17333601

([7]) EESK atzinums "Drošas informācijas sabiedrības stratēģija", OV C 97, 28.4.2007., 21. lpp.
EESK atzinums "Informācijas kritiskās infrastruktūras aizsardzība", OV C 255, 22.9.2010., 98. lpp.
EESK atzinums "*ENISA* regula", OV C 107, 6.4.2011., 58. lpp.
EESK atzinums "Vispārīgā datu aizsardzības regula", OV C 229, 31.7.2012., 90. lpp.
EESK atzinums "Uzbrukumi informācijas sistēmām", OV C 218, 23.7.2011., 130. lpp.
EESK atzinums "Elektronisko darījumu veikšana iekšējā tirgū", OV C 351, 15.11.2012., 73. lpp.
EESK atzinums "Mākoņdatošanas potenciāla atraisīšana Eiropā", OV C 76, 14.3.2013., 59. lpp.

2.4 Patlaban spēju un gatavības līmenis dalībvalstīs ir ļoti atšķirīgs, tāpēc Eiropas Savienībā vērojama TID nostādņu neviendabība. Tā kā tīkli un sistēmas ir savstarpēji savienotas, dažu dalībvalstu nepietiekamais aizsardzības līmenis vājina visas Savienības TID. Šādā situācijā kavēta ir arī dalībnieku savstarpējās uzticības veidošanās, kas ir priekšnoteikums sadarbībai un informācijas apmaiņai. Tādējādi sadarbība izveidojusies tikai starp tām nedaudzajām dalībvalstīm, kuru spējas ir augstā līmenī.

2.5 Saskaņā ar LESD 114. pantu ierosinātās direktīvas mērķis ir veicināt digitālā vienotā tirgus izveidi un nodrošināt netraucētu tā darbību, izmantojot šādus instrumentus:

— obligāta minimālā TID līmeņa noteikšana dalībvalstīs, tādējādi uzlabojot vispārējo sagatavotības un reaģēšanas uz incidentiem līmeni;

— ES līmeņa sadarbības uzlabošana TID jautājumos, lai apkarotu pārrobežu incidentus un apdraudējumus;

— riska pārvaldības kultūras veidošana un kvalitatīvāka informācijas apmaiņa starp privāto un publisko sektoru.

2.6 Direktīvas priekšlikumā noteiktas tiesiskās prasības, tostarp šādas:

a) katrai dalībvalstij jāpieņem TID stratēģija un jāieceļ par tīklu un informācijas sistēmu drošību atbildīgā valsts kompetentā iestāde, kuras rīcībā būtu pietiekami finanšu un cilvēkresursi, lai novērstu TID apdraudējumus un reaģētu uz incidentiem;

b) dalībvalstu un Komisijas sadarbības mehānisma izveide, lai apmainītos ar agrīniem brīdinājumiem par riskiem un incidentiem, sadarbotos un organizētu regulāras salīdzinošās izvērtēšanas;

c) prasība noteiktu veidu struktūrām visā ES pieņemt riska pārvaldības paņēmienus un ziņot attiecīgās valsts kompetentajai iestādei par būtiskiem savu pamatpakalpojumu drošības incidentiem. Minētās prasības attiektos uz kritisko informācijas infrastruktūru operatoriem atsevišķās nozarēs (finanšu pakalpojumi, transports, enerģētika, veselības aprūpe), informācijas sabiedrības pakalpojumu sniedzējiem (mākoņdatošana, e-tirdzniecības platformas, maksājumi internetā, meklētājprogrammas, lietojumprogrammu iegādes vietnes un sociālie tīkli), kā arī valsts pārvaldes iestādēm.

2.7 Dalībvalstīm jāievieš minētā direktīva ne vēlāk kā 18 mēnešus pēc tam, kad to pieņems Padome un Eiropas Parlaments (paredzēts 2014. gadā).

3. **Vispārīgas piezīmes**

3.1 Interneta un digitālās sabiedrības attīstība dziļi ietekmē mūsu ikdienu. Taču, pieaugot mūsu atkarībai no interneta, mūsu brīvība, pārticība un dzīves kvalitāte aizvien vairāk kļūst atkarīga no stabilas tīklu un informācijas drošības: ja internets nedarbojas un ārkārtas situācijā nav pieejami elektroniskie slimības vēstures dati, cilvēks ies bojā. Eiropas informācijas kritiskās infrastruktūras drošība tiek arvien vairāk apdraudēta, un mūsu TID līmenis nav pietiekami augsts.

3.2 *Europol* direktors pagājušajā gadā norādīja, ka ir ļoti noraizējies par šo nepareizo priekšstatu — pārliecību, ka internets ir neuzlaužams ([8]). Bieži nākas dzirdēt par noziedznieku, teroristu vai ārzemju valdību kārtējiem kiberuzbrukumiem būtiski svarīgai infrastruktūrai. Upuri par uzbrukumiem ziņo reti, jo nevēlas bojāt savu reputāciju. Tomēr vēl pirms dažām nedēļām izskanēja ziņas par uzbrukumiem Eiropas interneta infrastruktūrai ([9]) un banku sistēmām ([10]); kaitējums bija pārāk liels, lai to varētu noklusēt. Vienā no ziņojumiem aprēķināts ([11]), ka 2011. gadā Nīderlande pieredzējusi 92 miljonus kiberuzbrukumu, bet Vācija — 82 miljonus. Apvienotās Karalistes valdība lēš, ka 2011. gadā valsts piedzīvojusi 44 miljonus kibernoziedznieku uzbrukumu un ka tautsaimniecībai tie izmaksājuši līdz pat 30 miljardiem euro ([12]).

3.3 ES Padome Eiropas TID problēmai pievērsās 2007. gadā ([13]). Tomēr kopš tā laika īstenotā politikas pieeja ([14]) galvenokārt bijusi balstīta uz dalībvalstu brīvprātīgu rīcību, un tikai dažas no tām ir veikušas iedarbīgus pasākumus. Komiteja norāda, ka daudzas dalībvalstis vēl nav nedz publicējušas savu kiberdrošības stratēģiju, nedz sagatavojušas valsts līmeņa ārkārtas rīcības plānu kiberincidentu gadījumiem; dažas vēl nav izveidojušas Datorapdraudējumu reaģēšanas vienību (*CERT*). Turklāt vairākas dalībvalstis joprojām nav ratificējušas Eiropas Padomes konvenciju par kibernoziegumiem ([15]).

([8]) http://forumblog.org/2012/05/what-if-the-internet-collapsed/
([9]) http://www.nytimes.com/2013/03/27/technology/internet/online-dispute-becomes-internet-snarling-attack.html?pagewanted=all&_r=0
([10]) http://www.dutchnews.nl/news/archives/2013/04/online_retailers_demand_banks.php
([11]) http://www.securelist.com/en/analysis/204792216/Kaspersky_Security_Bulletin_Statistics_2011
([12]) "*UK Cyber Security Strategy: Landscape Review*" ("AK Kiberdrošības stratēģija — vispārējā stāvokļa apskats", http://www.nao.org.uk/wp-content/uploads/2013/03/Cyber-security-Full-report.pdf
([13]) Padomes rezolūcija 2007/C 68/01.
([14]) COM(2006) 251 un COM(2009) 149.
([15]) http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG

3.4 Desmit TID jomā augsti attīstītas dalībvalstis ir izveidojušas Eiropas Valdību *CERT* grupu (*EGC*), lai varētu cieši sadarboties saistībā ar TID un reaģēšanu uz incidentiem. Dalība grupā patlaban ir slēgta; šajā elitārajā apvienībā nevar iesaistīties ne pārējās mazāk attīstītās 17 dalībvalstis, ne jaunizveidotā *CERT-EU* ([16]). Veidojas jauna digitālā plaisa starp tām dalībvalstīm, kuras TID jomā ir augsti attīstītas, un pārējām. Ja šī plaisa netiks mazināta, TID atšķirības dos tiešu triecienu digitālajam vienotajam tirgum, jo tiks apgrūtināta uzticēšanās, saskaņotība un sadarbspēja. Turklāt, ja nebūs stingras rīcības, var pieaugt gan nošķirtība starp augsti attīstītajām un mazāk attīstītajām dalībvalstīm, gan iekšējā tirgus problēmas, kuru pamatā ir atšķirīgās dalībvalstu spējas.

3.5 Kiberdrošības stratēģijas un ierosinātās TID direktīvas iedarbīgums būs atkarīgs no tā, vai Eiropā būs spēcīga TID nozare un vai būs pietiekami daudz darbinieku ar specializētām TID prasmēm. EESK ir gandarīta, ka ierosinātajā direktīvā ir ņemta vērā vajadzība dalībvalstīs veikt ieguldījumus TID izglītībā, izpratnē par to un attiecīgā apmācībā. Komiteja vēlētos arī, lai ikviena dalībvalsts pieliktu īpašas pūles un kiberdrošības jautājumos informētu, izglītotu un atbalstītu MVU sektoru. Lielajiem uzņēmumiem iegūt nepieciešamās zināšanas ir viegli, bet mazajiem un vidējiem vajadzīgs atbalsts.

3.6 EESK labprāt sadarbosies ar Eiropas Tīklu un informācijas drošības aģentūru (*ENISA*), lai šogad plānotajā Kiberdrošības mēnesī popularizētu TID. Attiecībā uz kiberdrošības stratēģijas un TID direktīvas mērķi visā Savienībā attīstīt drošības jautājumu izpratnes kultūru un lai paaugstinātu TID prasmju līmeni, Komiteja vērš Komisijas uzmanību uz dažās dalībvalstīs un ASV notiekošo pusaudžiem domāto "hakeru konkursu" pozitīvo lomu izpratnes palielināšanā.

3.7 Komiteja atzinīgi vērtē arī to, ka kiberdrošības stratēģijā vērojama apņemšanās TID tehnoloģijai veltīt daļu no līdzekļiem, kas paredzēti pētniecībai, attīstībai un inovācijai.

3.8 Jaunus draudus kiberdrošībai rada mākoņdatošanas pieaugums. Piemēram, kibernoziedzniekiem patlaban ir pieejama ļoti liela datorjauda ar salīdzinoši zemām izmaksām, un tūkstošiem uzņēmumu savus datus tagad glabā centralizētās datu bāzēs, kas ir neaizsargātas pret labi izplānotiem uzbrukumiem. EESK jau ir aicinājusi palielināt mākoņdatošanas kibernoturīgumu ([17]).

([16]) *CERT-EU* ir pastāvīga ES iestāžu, aģentūru un struktūru Datorapdraudējumu reaģēšanas vienība (*CERT*).

([17]) EESK atzinums "Mākoņdatošana (*cloud computing*) Eiropā", OV C 24, 28.1.2012., 40. lpp., un "Mākoņdatošanas potenciāla atraisīšana Eiropā", OV C 76, 14.3.2013., 59. lpp.

3.9 Attiecībā uz darījumiem tiešsaistē Komiteja jau agrāk ir aicinājusi ieviest brīvprātīgu ES elektroniskās identifikācijas sistēmu, kas papildinātu jau izveidotās dalībvalstu shēmas. Tāda sistēma nodrošinātu labāku aizsardzību pret krāpšanu, ekonomikas dalībnieku lielāku savstarpējo uzticēšanos, zemākas pakalpojumu sniegšanas izmaksas, kvalitatīvākus pakalpojumus un iedzīvotāju aizsardzību.

4. **Īpašas piezīmes**

4.1 Diemžēl Komisijas ierosinātajai TID direktīvai pārāk lielā mērā piemīt pagaidu risinājuma iezīmes, tai trūkst skaidrības un vērojama pārlieka paļaušanās uz dalībvalstu pašregulējumu. Standartu, skaidru definīciju un kategorisku prasību trūkums, sevišķi direktīvas IV nodaļā, dod dalībvalstīm pārāk daudz iespēju atšķirīgi interpretēt un transponēt tiesību akta būtiskākos elementus. Iedarbīgāka par direktīvu būtu regula, kurā dalībvalstīm būtu paredzētas skaidri noteiktas, obligātas juridiskas saistības.

4.2 Komiteja norāda, ka direktīvas 6. pantā noteikta prasība katrai dalībvalstij iecelt kompetentu iestādi, lai visā ES uzraudzītu un kontrolētu, cik konsekventi direktīvu piemēro. Turklāt 8. pantā paredzēts sadarbības tīkls, kas saskaņā ar savām un Komisijas pilnvarām nodrošinās vadību Eiropas līmenī un vajadzības gadījumā arī ieviešanu dalībvalstīs. EESK uzskata, ka, pamatojoties uz šo pārvaldības sistēmu, Eiropas Savienībai būtu jāapsver iespēja izveidot ES līmeņa TID iestādi, kas būtu analoga Eiropas Aviācijas drošības aģentūrai (*EASA*), kura nosaka standartus un pārrauga drošības prasību ievērošanu attiecībā uz gaisa kuģiem, lidostām un aviosabiedrību darbību.

4.3 ES līmeņa TID iestādi, ko Komiteja ierosina šā atzinuma 4.2. punktā, varētu izveidot, pamatojoties uz darbu, ko kiberdrošības jomā jau paveikusi *ENISA*, Eiropas Standartizācijas komiteja (*CEN*), Datorapdraudējumu reaģēšanas vienības (*CERTs*), Eiropas Valdību *CERT* grupa (*EGC*) un citi. Šāda iestāde izstrādātu standartus un uzraudzītu visu TID aspektu īstenošanu — no drošu termināliekārtu sertifikācijas un lietošanas līdz tīkla un datu drošībai.

4.4 Tā kā TID nodrošināšanā visā Savienībā dalībvalstis ir ļoti atkarīgas cita no citas un TID problēmas visām iesaistītajām pusēm var izmaksāt ļoti dārgi, EESK vēlētos, lai tiesību aktā būtu proporcionālas un precīzi noteiktas sankcijas par prasību neievērošanu un lai tās būtu saskaņotas tā, ka atspoguļotu Eiropas dimensiju attiecībā uz atbildību un zaudējumu apmēru, kuri potenciāli varētu rasties ne tikai vietējā tirgū, bet arī visas Savienības mērogā. Tiesību akta 17. pants par sankcijām ir vispārīgs, un sankciju noteikšanā pārlieku daudz rīcības brīvības atstāts dalībvalstīm, kā arī nav pietiekamu norāžu par pārrobežu un Eiropas mēroga ietekmes izvērtēšanu.

4.5 Šobrīd valdības un pamatpakalpojumu sniedzēji nepublisko informāciju par kļūmēm, kas saistītas ar drošību un noturību, ja vien nav spiesti to darīt. Šāda informācijas nepieejamība negatīvi ietekmē Eiropas spēju ātri un efektīvi reaģēt uz kiberapdraudējumiem, kā arī kavē vispārējo TID uzlabošanu, mācoties vienam no otra. Komiteja aicina Komisiju pieņemt lēmumu ieviest direktīvā obligātu prasību ziņot par visiem būtiskiem TID incidentiem. EESK neuzskata, ka brīvprātīga ziņošana būs efektīva, jo, baidoties par reputāciju un atbildību, ir tendence slēpt negadījumus.

4.6 Tomēr direktīvas 14. pantā par paziņošanu nav definēts, ko nozīmē drošību būtiski ietekmējošs incidents, un attiecīgajām struktūrām un dalībvalstīm atstāts pārāk daudz rīcības brīvības lemt, vai par TID incidentu ziņot vai nē. Lai tiesību akts būtu iedarbīgs, tā prasībām jābūt nepārprotamām. Ierosinātajā direktīvā prasību būtība definēta pārāk vispārīgi, tāpēc iesaistītajām pusēm nevar piemērot sankcijas par noteikumu neievērošanu, kā paredzēts direktīvas 17. pantā.

4.7 Tā kā TID nodrošināšana ir galvenokārt privātā sektora pārziņā, ir būtiski, lai starp visiem uzņēmumiem, kas atbild par vitāli svarīgo informācijas infrastruktūru un pakalpojumiem, valdītu stabila uzticība un cieša sadarbība. Ļoti atzinīgi vērtējama un atbalstāma ir Eiropas publiskā un privātā sektora partnerība infrastruktūru noturības jautājumos (*EP3R* iniciatīva), kuru Komisija uzsāka 2009. gadā. Komiteja tomēr uzskata, ka minētā iniciatīva ir jāpapildina ar TID tiesību aktā noteiktu obligātu prasību sadarboties tām galvenajām iesaistītajām pusēm, kas to nedara pietiekami.

4.8 Ikvienai dalībvalstij būtu jāpublicē tiešsaistē pieejams saraksts ar visām tās jurisdikcijā esošajām struktūrām, uz kurām attiecas ierosinātās direktīvas 14. panta drošības prasības un pienākums paziņot par incidentiem. Šāda pārredzamība ne tikai viestu lielāku skaidrību par to, kā katra dalībvalsts piemēro 3. panta definīcijas, bet nostiprinātu arī iedzīvotāju uzticēšanos un sekmētu riska pārvaldības kultūras izveidi sabiedrībā.

4.9 EESK norāda, ka uz programmatūras izstrādātājiem un aparatūras ražotājiem direktīvas prasības nav attiecinātas, jo tie nav informācijas sabiedrības pakalpojumu sniedzēji. Tomēr, pēc Komitejas domām, ierosinātajā tiesību aktā būtu jānorāda, ka struktūras, uz kurām attiecas direktīvā noteiktās saistības, var vērsties ar prasību pie programmatūras vai aparatūras piegādātāja, ja tā izstrādājumiem vai pakalpojumiem bijuši defekti, kuri kļuvuši par TID incidentu tiešu cēloni.

4.10 Lai gan Komisija lēš, ka ierosinātās TID direktīvas īstenošana gadā izmaksās ap 2 miljardiem euro un ka šī summa attiecas uz visas Eiropas publisko un privāto sektoru kopā, Komiteja norāda, ka dažām finansiālās grūtībās nonākušām dalībvalstīm nebūs viegli rast līdzekļus, ko ieguldīt prasību izpildē. Ir jādomā, kā daudzgadu finanšu shēmā varētu paredzēt atbalstu TID prasību ievērošanai, šim nolūkam izmantojot dažādus instrumentus, piemēram, Eiropas Reģionālās attīstības fondu (ERAF) un, iespējams, Iekšējās drošības fondu.

Briselē, 2013. gada 22. maijā

Eiropas Ekonomikas un sociālo lietu komitejas priekšsēdētājs

Henri MALOSSE